Who Has Your Numbers?

It's time to try some methods of SELF-DEFENSE.

By Diane A. Riordan, CMA, CPA, and Michael P. Riordan, CPA

Two recent security failures have ratcheted up our fear of identity theft. On February 18 a hacker cherry-picked eight million credit card account numbers from a company that processes transactions for merchants. The cards included American Express, Discover, Visa, and MasterCard. Last November, federal prosecutors announced the nation's largest known case of identity theft involving 30,000 stolen credit histories. A crime ring used the histories to take over the victims' identities and then request credit cards, checks, and debit cards. One person reported a $34,000 loan taken out in her name. Overall losses are estimated to be at least $2.7 million and growing. According to U.S. Attorney James Comey, "With a few keystrokes, these men picked the pockets of tens of thousands of Americans and, in the process, took their identity, stole their money, and swiped their security."

Even before these historic cases of identity theft, a personal experience left us wondering about the safety of our own information. Shortly after we returned from a vacation in San Juan, Puerto Rico, a representative of our credit card company called. The inquiry was triggered by a sequence of events. According to the representative, someone in Brooklyn, N.Y., had changed our home address and subsequently requested a PIN number. The behavior pattern was caught by controls at the credit card company, and, fortunately, the card issuer was able to prevent misuse of our credit card.

More recently, we vacationed at Hilton Head long enough to require a few trips to the grocery store. We supplied a great deal of personal information to the clerks at the service desk, obtained a discount card, and enjoyed some savings. As we drove away from the store, we recalled our earlier post-vacation experience and questioned whether or not it was worth it to have surrendered our personal information.

Like most Americans, our awareness of identity fraud is growing. A *Wall Street Journal*-NBC poll identified privacy as Americans' number one concern for the 21st Century, and the General Accounting Office (GAO) reports a five-fold increase in allegations of Social Security number fraud from 1998 to mid-2001.

Reflecting the nation's ongoing concern, at least 50 bills concerning information privacy were introduced in Congress last year. Representative Cliff Stearns (R.-Fla.) sponsored the Consumer Privacy Protection Act in May 2002. It would place requirements on data-collection organizations and provide remedies in the case of identity fraud. In January 2003, Senators Dianne Feinstein (D.-Calif.), Jon Corzine (D.-N.J.), Charles Grassley (R.-Iowa), and Judd Gregg (R.-N.H.) introduced the Identity Theft Prevention Act.

Also in January, Senators Feinstein, Gregg, and Patrick Leahy (D.-Vt.) introduced the Social Security Number Misuse Prevention Act. The law would permit legitimate business and government use of Social Security numbers, but it would ban the sale and display of the numbers "without the expressed consent of the individual." The government would be prohibited from displaying Social Security numbers on "public records posted on the Internet or issued to the public through electronic media." And the bill "would limit when businesses may require customers to provide their Social Security numbers." In February, a bill to limit the misuse of Social Security numbers was again introduced in the House. This version of the Social Security Misuse Prevention Act was sponsored by Representative John Sweeney (R.-N.Y.).

Because your information is so widely stored, there's only so much you can do to *protect yourself*. The rest is a matter of *luck*.

WHO HAS YOUR PERSONAL INFORMATION?

We have put together a general list, but you may need to add items to reflect your personal situation. Don't forget to multiply by the number of times you have moved or otherwise changed business providers (see sidebar).

Personal information isn't only stored in computers but also in old file cabinets, discarded boxes, and the landfill. For example, what happened to the paper form that we submitted to the clerks at the grocery store? Recently, the Department of Labor of a large state reportedly sold some computers with personal information stored that should have been erased before the surplus sale. Someone forgot that when you "delete" data from a disk or drive, it's actually still there—some of it can even survive a formatting of the disk. And personal information may be transferred unintentionally through human error. No controls are 100% safe, and we're all at risk, especially if employees of companies that use our information violate our trust.

Recently, credit card statements have included offers to notify consumers, for a monthly fee, when someone requests credit on their record. Ironically, subscribing to such a service to track the use of personal information will result in adding still another organization to the list in the sidebar. Companies are also marketing identity theft insurance. It was just a matter of time before privacy itself became a mail-order business.

What can you do to protect yourself? Monica Favia, business instructor at Bloomsburg University, compares the risk of having your identity stolen with that of being hit by lightning. Because your information is so widely

stored, there's only so much you can do to protect yourself. The rest is a matter of luck.

This list of defensive behaviors will decrease your chances of being struck by identity fraud:

1. Use your Social Security number only when absolutely required. If you live in a state that formerly had your Social Security number as your license number, take advantage of the option to request a new license number. A colleague recently gave me his vita to file with the university's Curriculum and Instruction Board. It included his Social Security number; I deleted the number before forwarding it.

2. Don't give your Social Security number or any other personal information over the telephone unless you initiate the contact. When the bank contacted us about suspected credit card misuse, we insisted on calling them back to continue our discussions.

3. When initiating new business contacts that collect personal information, ask the company in writing not to share your personal information in unrelated transactions. Take advantage of the notices these companies will send to you offering to limit information sharing.

Organizations With Your *Personal Information*

How many of these organizations have your personal information?

- Armed Forces
- Banks
- Brokerage Firms
- City or County Commissioners of Revenue
- Colleges
- Continuing Professional Education Providers
- Credit Bureaus
- Credit Card Companies
- Department of Motor Vehicles
- Doctors, Dentists, Hospitals, Labs, and other medical providers
- Employers, Former Employers, and Potential Employers (applications on file)
- Finance Companies
- Grocery Stores (customer check-cashing and other clubs)
- Health Clubs
- Health Insurers
- Internal Revenue Service
- Investment Service Providers
- Landlords
- Lawyers
- Life Insurance Companies
- Loan Companies
- Mutual Funds
- Occupational and Professional Bureaus (for example, Boards of Accountancy)
- Libraries
- Realtors
- Retail Stores
- Retirement Plans
- School Systems
- Social Security Administration
- State Commissioners of Revenue
- U.S. State Department (for example, passport applications)
- Utility Companies
  - Telephone (local, long distance, and wireless accounts)
  - Fuel Oil and Gas
  - Electricity
- Voter Registrars

4. Safeguard your incoming and outgoing mail.

5. Buy a shredder for your use at home, and use it regularly after sorting the mail or paying your monthly bills. (A cross-cut shredder offers more security than a straight-cut shredder.)

6. Don't routinely carry your Social Security card.

7. Protect the copies of your charge slips.

8. Report lost cards immediately.

9. If you store personal information on your computer, safeguard it with firewalls and passwords.

10. Keep passports and other vital records in vaults. Otherwise, burglars, repair people, contractors, or household workers have access. Even family members and close friends can misuse your personal information.

11. Seclude yourself when transmitting vital information by telephone.

12. When using the cards provided by the Post Office for notifying them of an address change, put the postcard in an envelope, especially when an account number is provided.

13. Support legislation to protect personal information. Numerous bills have been introduced in Congress. Meaningful legislation is urgently needed.

14. Monitor your credit report. Reports are available from the three major credit reporting agencies: Equifax, Experian, and TransUnion.

15. Cross your fingers.

WHAT IS THE RISK IN YOUR COMMUNITY?

A survey of our IMA chapter and follow-up conversation at our professional meeting uncovered some interesting stories. One member believes his numbers were copied when he let his credit card out of his sight to pay a restaurant tab. Another reported leaving both charge slips on the table and the tip blank. The waiter helped himself to a big tip. About our personal experience, we've speculated whether it was the hotel, restaurant, or car rental company employees who shared our credit card information. The hotel employees in Puerto Rico did request a second imprint of our card when we checked out because they said they lost the first copy. In hindsight, we should have asked to record the incident with the manager.

One member inadvertently left his banking access card in an ATM, and the next user made a withdrawal. The wife of another member has the same name (absent her middle initial) as a local woman with a bad credit history. Giving another meaning to the phrase "the other woman," our friends have been contacted by mistaken creditors 23 times. Another professional reported leaving a purse unattended and later receiving unauthorized credit charges.

One of the 73 respondents reported the fraudulent submission of an application for a credit card on his credit record. Eleven percent reported an experience in the same category as ours—someone using their credit card numbers to try to transact business without having possession of the card itself. Fourteen percent reported unauthorized use of a credit card after losing control of it. In all, 23% reported at least one incident of crime.

Recent legislation has led insurance companies, financial institutions, and other data-collection organizations to mail out leaflets describing their policies on information sharing and our right to opt out. Yet few of us will take the time to respond to these offers to limit the transfer of certain personal information. It may seem the equivalent of sticking your finger into the leaking dike.

The recommended action for victims of identity theft is to file a police report, contact credit card companies, and call each of the three major credit bureaus: Experian, (888) 397-3742 (www.experian.com); TransUnion, (800) 680-7289 (www.transunion.com); and Equifax, (800) 685-1111 (www.equifax.com) to request that fraud alerts be placed on your credit reports. Also contact local credit bureaus. With file notations, consumers should be notified before new credit is issued. You can request long-term fraud alerts with credit bureaus in writing. Additional information for coping with identity theft has been posted by the Federal Trade Commission at www.ftc.gov.

Ironically, one of the individuals accused of the recent theft of at least 30,000 credit histories is a former employee of a company that provides computerized access to banks and other lending agencies to get commercial credit information from the three major credit bureaus. Given our current exposure, it's time to consider placing the burden on the credit bureaus to contact us each time they provide our reports to others. Until then, the lack of consumer control over personal information is the equivalent of crossing your fingers during a lightning storm. ■

Diane A. Riordan, CMA, CPA, and Michael P. Riordan, CPA, are professors of accounting at James Madison University in Harrisonburg, Va. You can reach them by e-mail at riordada@jmu.edu (for Diane) and riordamp@jmu.edu (for Michael).